AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method, comprising:
storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;
making the stored secret available at a first apparatus without contemporaneous user input; and
creating in the second apparatus, using the secret, a secret key for use in pairing the first and second apparatus to secure ~~securing~~ communication between ~~the first and second apparatus~~ them.

2. (Previously Presented) The method as claimed in claim 1, wherein the secret is previously generated at the second apparatus by user input to the second apparatus.

3. (Currently Amended) The method as claimed in claim 1, ~~wherein the stored secret is associated with an operational mode of the second apparatus~~ wherein the operational mode comprises a game mode.

4. (Previously Presented) The method as claimed in claim 1, wherein the stored secret is associated with a service provided by the second apparatus.

5. (Currently Amended) The method as claimed in claim 1, further comprising, at the second apparatus, receiving a signal from the first apparatus;
determining that the signal is associated with the operational mode of the second apparatus; and

in response to the ~~received signal~~ determining, automatically creating without user intervention, the secret key.

6. (Previously Presented) The method as claimed in claim 1, where making the stored secret available at the first apparatus is without communication in the radio communications network.

7. (Currently Amended) The method as claimed in claim 1, wherein making the stored secret available at the first apparatus involves prompting a user input of the secret ~~to~~ at the first apparatus.

8. (Previously Presented) The method as claimed in claim 1 further comprising storing in the second apparatus an identifier of the first apparatus and an identifier of the second apparatus.

9. (Previously Presented) The method as claimed in claim 1, wherein creating the secret key uses a random number communicated between the first and second apparatus.

10. (Previously Presented) The method as claimed in claim 1, wherein creating the secret key uses an identifier of one of the first and second apparatus, communicated between the first and second apparatus, in the creation of the secret key.

11. (Currently Amended) The method as claimed in claim 1, further comprising:
re-using the stored secret to join a third apparatus to a radio communications network without contemporaneous user input of a secret at the second apparatus, comprising:
making the stored secret available at the third apparatus; ~~and~~
creating in ~~the third apparatus and in~~ the second apparatus, using the secret, a secret key ~~for securing communication between the third and second apparatus~~; and
making the secret key available to the third apparatus for use in pairing the third and second

apparatus to secure communication between them.

12. (Currently Amended) A method, comprising:
storing in a second apparatus which controls access to a radio communications network a generated secret at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;
making the stored secret available to each of at least one or more first apparatus; and
creating in the second apparatus, using the secret, at least one secret key for use in pairing the one or more first apparatus and the second apparatus to secure ~~securing~~ communication between ~~the first apparatus and the second apparatus~~ them.

13. (Previously Presented) The method as claimed in claim 12, wherein the step of creating at least one secret key comprises:
creating a plurality of secret keys distributed across the first apparatus by creating a different secret key at each of the at least one or more first apparatus; and creating an identical plurality of secret keys at the second apparatus.

14. (Currently Amended) An apparatus comprising:
a user interface configured to generate a secret by user input;
a memory configured to store a generated secret for use in securing communications in a radio communications network comprising the apparatus and one or more additional apparatus, wherein the stored secret is associated with an operational mode of the apparatus;
a radio transceiver configured to communicate in the network; and
a processor configured to access the secret stored in the memory and to create, using the accessed secret, a secret key for use in pairing the apparatus and the one or more additional apparatus to secure ~~securing~~ communication between them.

15. (Currently Amended) The apparatus as claimed in claim 14, wherein the user interface is configured to generate the stored secret ~~is generated~~ by user input ~~using the user interface~~.

16. (Currently Amended) The apparatus as claimed in claim 14, ~~wherein the stored secret is associated with an operational mode of the apparatus~~ wherein the operational mode comprises a game mode.

17. (Previously Presented) The apparatus as claimed in claim 14, wherein the stored secret is associated with a service provided by the apparatus.

18. (Currently Amended) The apparatus as claimed in claim 14, wherein the radio transceiver is ~~operable~~ configured to receive a signal from any one of one or more additional ~~slave~~ apparatus;
the processor is configured to determine that the signal is associated with an operational mode of the apparatus; and
the processor is ~~operable~~ configured, in response to the determining, to access the secret in the memory ~~in response to the received signal~~ to create the secret key without user intervention.

19. (Previously Presented) The apparatus as claimed in claim 18, wherein the processor is operable to automatically create the secret key in response to the received signal.

20. (Previously Presented) The apparatus as claimed in claim 18, wherein the stored secret is independent of an origin of the received signal.

21. (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 18, wherein the secret key is dependent upon an origin of the received signal.

22. (Currently Amended) The apparatus as claimed in ~~claim 14~~ claim 18, wherein the received signal is a request and the secret key is dependent upon content of the received request.

23. (Previously Presented) The apparatus as claimed in claim 22, wherein the request

includes a random value used with at least the stored secret to create the secret key.

24. (Currently Amended) The apparatus as claimed in claim 14, wherein the processor is ~~operable~~ configured, in a first mode, to obtain a secret by accessing the secret stored in the memory, is ~~operable~~ configured, in a second mode, to obtain a secret by enabling user input of data, and is ~~operable~~ configured, in the first mode and in the second mode, to create, using the obtained secret, the secret key for use in pairing the apparatus and the one or more additional apparatus to secure ~~securing~~ communication between them.

25. (Previously Presented) The apparatus as claimed in claim 24, wherein the first mode is an interactive gaming mode and second mode is an idle mode.

26. (Previously Presented) The apparatus as claimed in claim 14, wherein the memory stores an apparatus identifier for use with at least the stored secret to create the secret key.

27. (Previously Presented) The apparatus as claimed in claim 14, further comprising a user input apparatus configured to program the value of the stored secret.

28. (Previously Presented) The apparatus as claimed in claim 14, wherein the secret key is for use in securing all communications in the network.

29. (Currently Amended) The apparatus as claimed in claim 14, wherein the memory is ~~for storing~~ configured to store a secret for use in securing communications in the network between the apparatus and a first additional apparatus and between the apparatus and a second additional apparatus, the processor is configured to access the secret in the memory and to create, using the secret, a first secret key in common with the first additional apparatus for use in pairing the apparatus and the first additional apparatus to secure ~~securing~~ communication between the apparatus and the first additional apparatus and a second secret key in common with the second additional apparatus for use in pairing the apparatus and the second additional apparatus to secure ~~securing~~ communication between the apparatus and the

second additional apparatus.

30. (Previously Presented) The apparatus as claimed in claim 14, further comprising a user interface configured to enable data entry, wherein when the apparatus participates in a different network controlled by a different apparatus the user interface is configured to enter a secret stored at the different apparatus and the processor is operable to create, using the entered secret, a secret key for securing communication.

31-33. (Canceled)

34. (Currently Amended) An apparatus comprising:
means for storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;
means for making the stored secret available at a first apparatus without contemporaneous user input; and
means for creating in the second apparatus, using the secret, a secret key for use in pairing the first apparatus and the second apparatus to secure communication between ~~the first and second apparatus~~ them.

35. (Currently Amended) A memory ~~storing~~ embodying a program of computer readable instructions that when executed ~~executable~~ by a processor ~~to~~ perform actions directed to securing communication between a first and second apparatus, the actions comprising:
storing in ~~a~~ the second apparatus which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret is associated with an operational mode of the second apparatus;
making the stored secret available at ~~a~~ the first apparatus without contemporaneous user input; and
creating in the second apparatus, using the secret, a secret key for use in pairing the first apparatus and the second apparatus to secure communication between ~~the first and second~~

~~apparatus~~ them.

36. (New) The memory embodying instructions executable by a processor of claim 35, wherein the operational mode comprises a game mode.

37. (New) The memory embodying instructions executable by a processor of claim 35 comprising,

receiving a signal, at the second apparatus, from the first apparatus;

determining that the signal is associated with the operational mode of the second apparatus; and

in response to the determining, automatically creating, without user intervention, the secret key.